数理解析研究所講究録 1200 巻 2001 年 149-161

An effective surjectivity of mod l Galois representation of 1- and 2-dimensional abelian varieties with trivial endomorphism ring

東大数理　河村隆 (Takashi Kawamura)

Graduate School of Mathematical Sciences,

University of Tokyo

1 Introduction and main results

Let A be a principally polarized abelian variety of dimension n over an algebraic number field K. For a prime l let A_l be the group of l-division points of A, which is a vector space of dimension $2n$ over $\mathbf{F}_l$. Let μ_l be the group of l-th roots of unity in the algebraic closure $\bar{K}$ of K, and let $\varepsilon_l: G_K := \mathrm{Gal}(\bar{K}/K) \to \mathbf{F}_l{}^* \cong \mathrm{Aut}(\mu_l)$ be the cyclotomic character. As A is principally polarized, the Weil pairing $W: A_l \times A_l \to \mu_l$, written additively, defines a symplectic form with $2n$ variables, satisfying $W(\sigma(P), \sigma(Q)) = \varepsilon_l(\sigma)W(P, Q)$ for $(P, Q) \in A_l \times A_l$ and $\sigma \in G_K$. Hence a Galois representation $\rho_l: G_K \to GSp_{2n}(\mathbf{F}_l)$ is obtained, where

$GSp_{2n}(\mathbf{F}_l)$ is the group of symplectic similitudes of dimension $2n$ with entries in $\mathbf{F}_l$.

Serre [1] proved that when $n = 2$, 6 or odd, and $\mathrm{End}_{\bar{K}}(A) = \mathbf{Z}$, ρ_l is surjective for sufficiently large l. The proof uses Faltings' theorem and standard theorems of algebraic groups. Though the result is general, it does not give an effective lower bound of l_0 such that ρ_l is surjective for $l > l_0$.

Le Duff [2] gives a sufficient condition for the surjectivity of ρ_l when $n = 2$ under some assumption on the reduction of abelian varieties. He also suggested that the explicit calculation of the constants in the refinement of Faltings' theorem by Masser and Wüstholz [3] should enable one to evaluate l_0 effectively. But no details are given.

The purpose of this paper is to supply an "elementary" proof of the surjectivity for $n = 1$ or 2, which also gives an effective evaluation of l_0. The proof uses Masser-Wüstholz theorem [3] and Kleidman and Liebeck's [4] detailed results about the classification of the maximal subgroups of the finite classical groups, especially of $GSp_2(\mathbf{F}_l) \cong GL_2(\mathbf{F}_l)$ and $GSp_4(\mathbf{F}_l)$.

Main Theorem 1. Let E be an elliptic curve over an algebraic number field K of degree d with $\mathrm{End}_{\bar{K}}(E) = \mathbf{Z}$. For a prime l let E_l be the group of l-division points of E, and let G_l be the image of the representation ρ_l of $G_K := \mathrm{Gal}(\bar{K}/K)$ on E_l. If $l > \max(49,\ |D(K)|,\ C(1)[\max\{2d,\ h(E)\}]^{\tau(1)})$, then $G_l = GL_2(\mathbf{F}_l)$, where $D(K)$ is the discriminant of K, $h(E)$ is the Faltings height of E, $C(1)$ is a constant $C(n)$ in Theorem 2 of Section 2 when $n = 1$, and $\tau(1)$ is the constant τ given in Theorem 1 of Masser and Wüstholz [3] when $n = 1$. Explicitly $\tau(1) = 2^{277} \cdot 3^4 \cdot 5^2 \cdot 136! \times (2^{276} \cdot 3^3 \cdot 5 \cdot 136! + 1)^7 + 2^{1066} \cdot 3 \cdot 7 \cdot 17 \cdot 19 \cdot 31 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! + 1)^{15}$.

Main Theorem 2. Let A be a two-dimensional principally polarized abelian variety over an algebraic number field K of degree d with $\mathrm{End}_{\bar{K}}(A) = \mathbf{Z}$. If $l > \max(3841,\ |D(K)|,\ C(2)[\max\{2d,\ h(E)\}]^{\tau(2)})$, then $G_l = GSp_4(\mathbf{F}_l)$, where $C(2)$ is a constant $C(n)$ in Theorem 2 of Section 2 when $n = 2$, and $\tau(2)$ is the constant τ given in Theorem 1 of Masser and Wüstholz [3] when $n = 2$. Explicitly $\tau(2) = 2^{1064} \cdot 17 \cdot 31^2 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! + 1)^{15} + 2^{4176} \cdot 3^6 \cdot 7^3 \cdot 11 \cdot 19 \cdot 2080! \times (2^{4166} \cdot 3^3 \cdot 7 \cdot 11 \cdot 2080! + 1)^{31}$.

2 Proof of Main Theorems

Masser and Wüstholz [5, Theorem II] (see also the note at the end of [5]) estimated the degree of an isogeny between abelian varieties over a number field effectively.

Theorem 1. Given positive integers n and d, there are constants $\kappa(n)$ and $C(n)$ depending only on n with the following property. Let A and A' be abelian varieties of dimension n defined over a number field K of degree d. Then if they are isogenous over K, there is an isogeny over K from A to A' of degree at most $C(n)[\max\{d,\ h(A)\}]^{\kappa(n)}$, where $h(A)$ is the Faltings height of A, which is invariant under extension of the ground field.

Using Theorem 1, they [3, Theorem 1] (see also the note at the end of [3]) refined Faltings' theorem in the following effective way.

Theorem 2. Given positive integers n and d, there are constants $\tau(n)$ and $C(n)$ depending only on n with the following property. Let A be an abelian variety of dimension n defined over a number field K of degree d. then there is a positive integer $M \leq C(n)[\max\{d,\ h(A)\}]^{\tau(n)}$ such that for any positive integer m the natural map $\mathrm{End}_K(A) \to \mathrm{End}_{G_K}(A_m)$ has cokernel killed by M.

Corollary. Suppose M as in Theorem 2. Then for any prime l not dividing M the natural map $\mathrm{End}_K(A) \otimes_{\mathbf{Z}} \mathbf{F}_l \to \mathrm{End}_{G_K}(A_l)$ is an isomorphism.

Explicitly $\tau(n) = n^2\lambda(8n) + 3\kappa(2n)$ by [3, Section 6], where $\lambda(n) = 4\mathrm{rank}_{\mathbf{Z}}\{\mathrm{End}_K(A)\}n(2n-1)k(n)\{2nk(n)+1\}^{n-1}$ by [6, Section 5], $k(n)$ being $(2n^2+n-1)4^{n(2n+1)}\{n(2n+1)\}!$, and $\kappa(n) = 10n^3\lambda(8n)+32n^2\mu(8n)$ by [5, Section 7], $\mu(n)$ being $[\mathrm{rank}_{\mathbf{Z}}\{\mathrm{End}_K(A)\}]^{-1}n\lambda(n)$ by [6, Section 6].

Let us recall another material. Aschbacher [7] obtained the classification theorem of the maximal subgroups of the finite classical groups. Kleidman and Liebeck [4] decided the structure of the maximal subgroups more precisely. After that the Main Theorem and Table 3.5.C of [4, Ch. 3, pp. 57, 70 and 72] imply the following Propositions about the maximal subgroups of $GL_2(\mathbf{F}_l)$ and $GSp_4(\mathbf{F}_l)$.

Proposition 1. When $l \geq 5$, a maximal subgroup of $GL_2(\mathbf{F}_l)$ is conjugate to one of the following five subgroups.

(1)$SL_2(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_1\rangle$),

(2)maximal parabolic subgroup,

(3)normalizer of the split Cartan subgroup $\cong \mathbf{F}_l{}^* \rtimes S_2 \rtimes \langle\delta_1\rangle$,

(4)normalizer of the nonsplit Cartan subgroup $\cong \mathbf{F}_{l^2}{}^* \bullet \mathbf{Z}_2$, and

(5)$Q_8 \bullet D_6$,

where δ_1 is the element expressed as diag$(\mu,\ 1)$ with respect to a basis of $\mathbf{F}_l{}^2$, μ being a generator of $\mathbf{F}_l{}^*$. For groups G and H, $G \bullet H$ denotes the extension of G by H. D_n is the dihedral group of order n, $\mathbf{Z}_2$ is the cyclic group of order 2, and Q_8 is the quaternion group.

Proposition 2. When $l \geq 3$, a maximal subgroup of $GSp_4(\mathbf{F}_l)$ is conjugate to one of the following seven subgroups.

(1)$Sp_4(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_2\rangle$),

(2)maximal parabolic subgroup,

(3)$SL_2(\mathbf{F}_l) \rtimes S_2 \rtimes \langle\delta_2\rangle$,

(4)$GL_2(\mathbf{F}_l) \bullet \mathbf{Z}_2 \rtimes \langle\delta_2\rangle$,

(5)$SL_2(\mathbf{F}_{l^2}) \rtimes \langle\delta_2\rangle$,

(6)$GU_2(\mathbf{F}_{l^2}) \rtimes \langle\delta_2\rangle$, and

(7)$D_8 \circ Q_8 \bullet O_4{}^-(\mathbf{F}_2)$,

where δ_2 is the element expressed as diag$(\mu,\ \mu,\ 1,\ 1)$ with respect to a symplectic basis of $\mathbf{F}_l{}^4$. $\circ$ denotes the central product, and $O_4{}^-$ is the

4-dimensional orthogonal group with defect 1.

Let ζ_l be a primitive l-th root of unity. If $K \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$, then ε_l is surjective. The condition on l is given by the following Lemma.

Lemma. If $l > |D(K)|$, then $K \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$.

Proof. The discriminant of $\mathbf{Q}(\zeta_l)$, $D(\mathbf{Q}(\zeta_l))$, is l^{l-2} when $l = 2$ or $\equiv 1 \pmod 4$, and $-l^{l-2}$ when $l \equiv 3 \pmod 4$. The discriminant of $K \cap \mathbf{Q}(\zeta_l)$ divides the greatest common divisor of $D(K)$ and $D(\mathbf{Q}(\zeta_l))$, which is 1 if $l > |D(K)|$. By Minkowski's theorem $K \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$. q. e. d.

Proof of Main Theorem 1. We prove that G_l is not contained in any maximal subgroups of $GL_2(\mathbf{F}_l)$ in Proposition 1.

As $l > |D(K)|$, ε_l is surjective by Lemma, so that $G_l \not\subset SL_2(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle \delta_1 \rangle$).

The Borel subgroup stabilizes a one-dimensional subspace W_1 of $V_1 := \mathbf{F}_l{}^2$. If G_l is contained in it, there is a K-isogeny $f : E \to E/W_1$ of degree l. By Theorem 1 it should be a composition of isogenies of degree at most $C(1)[\max\{d, h(E)\}]^{\kappa(1)}$, contradicting the fact that l is a prime.

Next if $G_l \subset \mathbf{F}_l{}^* \rtimes S_2 \rtimes \langle \delta_1 \rangle$, then there exists a surjective homomorphism φ from G_l to S_2. Let L be $\bar{K}^{\ker(\varphi\circ\rho_l)}$, then $[L : K] \leq 2$, and

$\rho_l(G_L := \mathrm{Gal}(\bar{K}/L)) \subset \mathbf{F}_l{}^* \rtimes \langle\delta_1\rangle$. Thus $\mathrm{End}_{G_L}(E_l) \supset \mathbf{F}_l{}^2$. On the other hand, as $l > C(1)[\max\{2d, h(E)\}]^{\tau(1)}$, $\mathrm{End}_{G_L}(E_l) \cong \mathrm{End}_L(E) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. This is a contradiction.

If $G_l \subset \mathbf{F}_{l^2}{}^* \bullet \mathbf{Z}_2$, then there exists a quadratic extension L' of K such that $\rho_l(G_{L'} := \mathrm{Gal}(\bar{K}/L')) \subset \mathbf{F}_{l^2}{}^*$. Thus $\mathrm{End}_{G_{L'}}(E_l) \supset \mathbf{F}_{l^2}$. On the other hand, as $l > C(1)[\max\{2d, h(E)\}]^{\tau(1)}$, $\mathrm{End}_{G_{L'}}(E_l) \cong \mathrm{End}_{L'}(E) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. Hence a contradiction.

Lastly assume that $G_l \subset Q_8 \bullet D_6$. As ε_l is surjective by Lemma, $|G_l| \geq |\mathbf{F}_l{}^*| = l - 1 > 48 = |Q_8 \bullet D_6|$. This is a contradiction.

When $\mathrm{End}_K(E) = \mathbf{Z}$, $\tau(1) = 2^{277} \cdot 3^4 \cdot 5^2 \cdot 136! \times (2^{276} \cdot 3^3 \cdot 5 \cdot 136! + 1)^7 + 2^{1066} \cdot 3 \cdot 7 \cdot 17 \cdot 19 \cdot 31 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! + 1)^{15}$.

Proof of Main Theorem 2. We prove that G_l is not contained in any maximal subgroups of $GSp_4(\mathbf{F}_l)$ in Proposition 2.

$G_l \not\subset Sp_4(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_2\rangle$), for ε_l is surjective.

Maximal parabolic subgroups stabilize a one- or two-dimensional subspace of $V_2 := \mathbf{F}_l{}^4$ [4, p. 72, Table 3.5.C]. So G_l is not contained in them similarly as the case of the Borel subgroup in Main Theorem 1.

$SL_2(\mathbf{F}_l) \rtimes S_2 \rtimes \langle\delta_2\rangle$ stabilizes a two-dimensional subspace of V_2. In fact, let $\{e_i | 1 \leq i \leq 4\}$ be a symplectic basis of V_2. Let $H := SL_2(\mathbf{F}_l) \rtimes S_2$,

$$H_0 := \left\{ \left(\begin{array}{cc|cc} a & 0 & b & 0 \\ 0 & a & 0 & b \\ \hline c & 0 & d & 0 \\ 0 & c & 0 & d \end{array} \right) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_l) \right\},$$

and

$$w := \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array} \right).$$

Then $H = H_0 \cup H_0 w$. We consider the action of H on $W_2 := \mathbf{F}_l(e_1 \oplus e_2) \oplus \mathbf{F}_l(e_3 \oplus e_4)$. For k_1 and $k_2 \in \mathbf{F}_l$

$$\left(\begin{array}{cc|cc} a & 0 & b & 0 \\ 0 & a & 0 & b \\ \hline c & 0 & d & 0 \\ 0 & c & 0 & d \end{array} \right) \begin{pmatrix} k_1 \\ k_1 \\ k_2 \\ k_2 \end{pmatrix} = \begin{pmatrix} ak_1 + bk_2 \\ ak_1 + bk_2 \\ ck_1 + dk_2 \\ ck_1 + dk_2 \end{pmatrix},$$

$$\left(\begin{array}{cc|cc} a & 0 & b & 0 \\ 0 & a & 0 & b \\ \hline c & 0 & d & 0 \\ 0 & c & 0 & d \end{array}\right)\left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)\begin{pmatrix} k_1 \\ k_1 \\ k_2 \\ k_2 \end{pmatrix} = \begin{pmatrix} ak_1 + bk_2 \\ ak_1 + bk_2 \\ ck_1 + dk_2 \\ ck_1 + dk_2 \end{pmatrix}.$$

So $H_0 W_2 \subset W_2$ and $H_0 w W_2 \subset W_2$. Thus W_2 is a nontrivial invariant subspace of V_2 under the action of H. As $\langle \delta_2 \rangle$ acts on $\mathbf{F}_l(e_1 \oplus e_2)$ by multiplication by scalars, and on $\mathbf{F}_l(e_3 \oplus e_4)$ trivially, W_2 is invariant also under the action of $H \rtimes \langle \delta_2 \rangle = SL_2(\mathbf{F}_l) \rtimes S_2 \rtimes \langle \delta_2 \rangle$. Thus $G_l \not\subset SL_2(\mathbf{F}_l) \rtimes S_2 \rtimes \langle \delta_2 \rangle$ similarly as the case of maximal parabolic subgroups.

$G_l \not\subset GL_2(\mathbf{F}_l) \bullet \mathbf{Z}_2 \rtimes \langle \delta_2 \rangle$ similarly as the case of $\mathbf{F}_l{}^* \rtimes S_2 \rtimes \langle \delta_1 \rangle$ in Main Theorem 1.

If $G_l \subset SL_2(\mathbf{F}_{l^2}) \rtimes \langle \delta_2 \rangle$ or $G_l \subset GU_2(\mathbf{F}_{l^2}) \rtimes \langle \delta_2 \rangle$, then G_l commutes with $\mathbf{F}_{l^2}$. On the other hand, as $l > C(2)[\max\{d, h(A)\}]^{\tau(2)}$, $\mathrm{End}_{G_K}(A_l) \cong \mathrm{End}_K(A) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. Hence a contradiction.

$G_l \not\subset D_8 \circ Q_8 \bullet O_4{}^-(\mathbf{F}_2)$ similarly as the case of $D_8 \circ Q_8$ in Main Theorem 1, for $|D_8 \circ Q_8 \bullet O_4{}^-(\mathbf{F}_2)| = 3840$.

When $\mathrm{End}_K(A) = \mathbf{Z}$, $\tau(2) = 2^{1064} \cdot 17 \cdot 31^2 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! +$

$1)^{15} + 2^{4176} \cdot 3^6 \cdot 7^3 \cdot 11 \cdot 19 \cdot 2080! \times (2^{4166} \cdot 3^3 \cdot 7 \cdot 11 \cdot 2080! + 1)^{31}$.

Remarks. (a) The effective dependence of $C(n)$ on the dimension n remains an interesting problem.

(b) When $\dim A = 3$, the classification of maximal subgroups of $GSp_6(\mathbf{F}_l)$ is also known [4, p. 72, Table 3.5.C]. When $l \geq 5$, they are

(1)$Sp_6(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle \delta_3 \rangle$),

(2)maximal parabolic subgroup,

(3)$SL_2(\mathbf{F}_l) \times Sp_4(\mathbf{F}_l) \rtimes \langle \delta_3 \rangle$,

(4)$SL_2(\mathbf{F}_l) \rtimes S_3 \rtimes \langle \delta_3 \rangle$,

(5)$GL_3(\mathbf{F}_l) \bullet \mathbf{Z}_2 \rtimes \langle \delta_3 \rangle$,

(6)$SL_2(\mathbf{F}_{l^3}) \rtimes \langle \delta_3 \rangle$,

(7)$GU_3(\mathbf{F}_{l^2}) \rtimes \langle \delta_3 \rangle$, and

(8)$SL_2(\mathbf{F}_l) \circ O_3(\mathbf{F}_l) \rtimes \langle \delta_3 \rangle$,

where δ_3 is the element expressed as $\mathrm{diag}(\mu, \mu, \mu, 1, 1, 1)$ with respect to a symplectic basis of ${\mathbf{F}_l}^6$. The first seven are handled similarly as the 2-dimensional case, for (3) is also reducible. Only the case (8) seems to be difficult to treat.

Acknowledgements. The author is most grateful to Professor Takayuki

Oda for helpful advice. He thanks Professor Jean-Pierre Serre for valuable comments. He is indebted to Dr. Akio Tamagawa for pointing out problems in the draft. He is grateful also to Dr. Fumio Sairaiji for reference to the paper [2].

References

[1] J.-P. Serre, Résumés des cours au Collège de France, Ann. Coll. France (1985-86), 95-99.

[2] P. Le Duff, Points d'ordre l des jacobiennes de certaines courbes de genre 2. C. R. Acad. Sci. Paris **325**, Série I (1997), 243-246.

[3] D. W. Masser and G. Wüstholz, Refinements of the Tate conjecture for abelian varieties, in: Abelian Varieties (W. Barth, K. Hulek and H. Lange, Eds.), Walter de Gruyter (1995), 211-223.

[4] P. Kleidman and M. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press (1990).

[5] D. W. Masser and G. Wüstholz, Factorization estimates for abelian varieties, Publ. Math. IHES **82** (1995), 5-24.

[6] D. W. Masser and G. Wüstholz, Endomorphism estimates for abelian

varieties, Math. Z. **215** (1994), 641-653.

[7] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math. **76** (1984), 469-514.